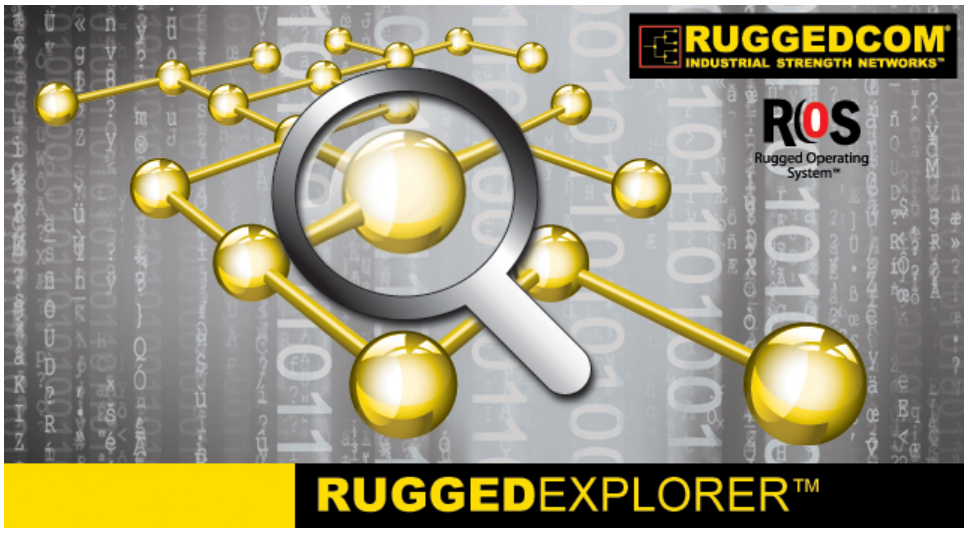
RuggedExplorer™

Version 1.1 User Guide



RuggedCom Inc.

30 Whitmore Road
Woodbridge, Ontario
Canada L4L 7Z4

Tel: (905) 856-5288
Fax: (905) 856-1995
Toll Free: (888) 264-0006

support@ruggedcom.com

RuggedExplorer™ Version 1.1 User Guide

Discovery tool for RuggedCom Networking Equipment

Version 1.1 - September 3, 2009

RuggedCom Inc.

30 Whitmore Road
Woodbridge, Ontario
Canada L4L 7Z4

Tel: (905) 856-5288
Fax: (905) 856-1995
Toll Free: (888) 264-0006

support@ruggedcom.com

Disclaimer

RuggedCom Inc. makes no warranty of any kind with regard to this material.

RuggedCom Inc. shall not be liable for errors contained herein or for consequential damages in connection with the furnishing, performance, or use of this material.

Warranty

This software comes with no warranty.

ALL RIGHTS RESERVED

This document contains proprietary information which is protected by copyright. All rights are reserved.

No part of this document may be photocopied, reproduced or translated to another language without the prior written consent of RuggedCom Inc.

Registered Trademarks

RuggedExplorer™, RuggedServer™, RCDP™, and RuggedCom Discovery Protocol™ are trademarks of RuggedCom Inc. ROS® and RuggedSwitch® are registered trademarks of RuggedCom Inc. Other designations in this manual might be trademarks whose use by third parties for their own purposes would infringe upon the rights of the owner.

Patent Information

RCDP™, the RuggedCom Discovery Protocol™, is U.S. patent pending.

Table of Contents

Preface 6
Foreword 6
Who Should Use RuggedExplorer 6
Document Conventions 6
More Information / Feedback 6
1. Introduction to RuggedExplorer™ 7
1.1. Purpose 7
1.2. Features 7
1.3. Use Cases 7
1.4. Installation Notes 8
1.5. Compatibility / Operating Requirements 8
2. User Interface 10
2.1. Initialization 10
2.2. Main Window 10
2.2.1. Main Window Display 10
2.2.2. Main Window Buttons 13
2.2.3. Main Window Menu Bar 14
2.3. Device Discovery 17
2.3.1. Auto Discovery 17
2.3.2. Manual Discovery 18
2.3.3. Rescanning Discovered Devices 20
2.4. Device Configuration 21
2.4.1. Single Device Configuration 21
2.4.2. Group Device Configuration 22
2.5. Device Control 24
2.5.1. Download 24
2.5.2. Upload 25
2.5.3. Maintenance 27
2.5.4. Progress Indication 27
3. Theory Of Operation 30
3.1. Device Discovery Methods 30
3.1.1. Automatic (RuggedCom Discovery Protocol™-based) Device Discovery 30
3.1.2. Manual (TCP/IP-based) Device Discovery 30
3.1.3. RCDP Versus TCP/IP Discovery Comparison 30
3.2. Security Considerations 31
3.3. Duplicate Instance Detection 31
A. RuggedExplorer.ini Configuration File 33
A.1. Auto Configuration Parameters 33
A.2. Logging Parameters 33
A.3. General Parameters 33
B. RuggedExplorer™ Software License 35
B.1. LICENSE 35
B.1.1. 35
B.1.2. 35
B.1.3. 35
B.1.4. 36

B.2. TITLE AND OWNERSHIP 36
B.2.1. 36
B.2.2. 36
B.2.3. 36
B.2.4. 37
B.3. LIMITED WARRANTY 37
B.3.1. 37
B.3.2. 37
B.3.3. 37
B.4. LIMITATION OF REMEDIES 37
B.4.1. 37
B.4.2. 38
B.5. INDEMNIFICATION 38
B.5.1. Indemnification In Favour Of Yourself 38
B.5.2. Indemnification In Favour Of RuggedCom 39
B.6. TERMINATION 39
B.7. GOVERNING LAW 39
B.8. ASSIGNMENT 40
B.9. RESTRICTED RIGHTS 40
B.10. ACKNOWLEDGEMENT 40
Index 41

List of Figures

2.1. Network Interface List Dialog Box 10
2.2. Main Window 10
2.3. Main Window Display Columns 12
2.4. Main Window Buttons 13
2.5. File Menu 14
2.6. Commands Menu 14
2.7. Table Menu 15
2.8. Filter Menu 15
2.9. View Menu 16
2.10. Auto Discovery Menu 16
2.11. Help Menu 17
2.12. Auto Discovery Access Dialog Box 18
2.13. Device Discovery Dialog Box 18
2.14. IP Address Range Discovery/Validation 20
2.15. Rescan Validation 21
2.16. Device Configuration Dialog Box 22
2.17. Group Configuration Dialog Box 23
2.18. File Download Dialog Box 24
2.19. File Upload Dialog Box 26
2.20. Device Maintenance Dialog Box 27
2.21. Progress Dialog Box (Processing in Progress) 28
2.22. Progress Dialog Box (Processing Complete) 28
2.23. Device Log 29
3.1. Detecting Another Instance Of RuggedExplorer On The LAN 32
3.2. Detecting Another Instance Of RuggedExplorer On The Same Computer 32

Preface

Foreword

This guide documents RuggedCom's RuggedExplorer™ software utility for the discovery, initial configuration and general maintenance of RuggedCom RuggedSwitch® and RuggedServer™ networking products.

Who Should Use RuggedExplorer

This software is intended to be used by technical support personnel who are familiar with the operation of data networks and with the configuration and deployment of ROS™-based products in particular. Others who might find RuggedExplorer useful are network and system planners and system programmers.

Document Conventions

This publication uses the following conventions:

Note

Means, "Reader take note". Notes contain helpful suggestions or references to materials not contained in this guide.

This document uses UTF-8 (Unicode) character encoding, and is available in both PDF and HTML formats.

More Information / Feedback

If you have questions or concerns about the contents of this guide or about the operation of RuggedExplorer, please contact RuggedCom at `support@ruggedcom.com`.

Other documents of interest regarding RuggedCom equipment relevant to RuggedExplorer are available at http://www.ruggedcom.com including:

- Rugged Operating System™ User Guide
- RuggedSwitch® Installation Guide

Please check http://www.ruggedcom.com periodically for updates to RuggedExplorer.

RuggedNMS™ is a fully-featured enterprise grade network management software platform designed specifically for the rugged communications industry. RuggedNMS provides a comprehensive platform for monitoring, configuring, and maintaining mission-critical IP-based communications networks, such as those found in substation automation and “Smart Grids” for electric utilities, intelligent transportation systems, and advanced control and automation for industrial processes.

For more information on RuggedNMS™ please visit http://www.ruggednms.com.

1. Introduction to RuggedExplorer™

1.1. Purpose

RuggedExplorer™ is a lightweight, standalone tool providing limited management capabilities of ROS™ devices. It allows a technician to discover, identify and configure all ROS-based devices. The tool will only allow for the configuration of a small number of parameters to be discussed in detail later in this document.

Using RuggedCom's proprietary Layer 2 RuggedCom Discovery Protocol™ (RCDP™), RuggedExplorer is able to discover and configure ROS-based devices irrespective of their IP network configuration, including no IP configuration at all.

RuggedExplorer's Automatic Discovery mode requires RCDP support to be present in devices to be discovered. This requires that devices be running ROS version 3.7 or newer. RCDP is enabled on ROS-based devices by default when they are shipped from the factory.

1.2. Features

- Automatic discovery of new, unconfigured RuggedCom devices running ROS™ version 3.7.0 or greater using RCDP over Ethernet.
- Manual discovery of RuggedCom devices running ROS versions prior to 3.7.0 using TCP/IP.
- Basic configuration of IP addressing and system identification parameters.
- Bulk firmware updating of multiple ROS-based devices.
- Summary display of discovered devices, their status and some basic parameters.
- Easy identification of devices via control of panel LEDs.

1.3. Use Cases

Some common uses of RuggedExplorer are:

- **Commissioning of new devices:** Using RCDP, RuggedExplorer allows a network of ROS devices to be commissioned in place in the network with no prior configuration necessary. It is capable of discovering and configuring ROS devices that have been taken directly from the factory and connected to the network.
- **Bulk configuration or reconfiguration:** RuggedExplorer can be used to modify the network and identification configuration parameters of one or multiple ROS devices, either one at a time, or using a template-based auto-incrementing tool.
- **Asset reporting:** RuggedExplorer can generate a report of ROS-based network device assets on a network segment. If RCDP is supported on all devices, RuggedExplorer need not have any prior knowledge of IP addressing used by ROS devices.
- **Network debugging:** RuggedExplorer can be used to report the occurrence of duplicate IP addresses, or of inconsistencies in IP address allocation among ROS devices. Note that RCDP support is required in order to detect certain IP addressing misconfigurations.
- **Bulk firmware upgrade:** RuggedExplorer can be used to upgrade the firmware of one or multiple devices at once.

- **System backup:** The configuration, firmware, log, and other ancillary files of one or multiple devices can be retrieved and archived in a single step.
- **Diagnostic data retrieval:** Diagnostic data (system logs and alarms) from one or multiple devices can be retrieved and archived in a single step.

1.4. Installation Notes

RuggedExplorer is a Java-based application with a graphical user interface that runs under Microsoft Windows. It has been tested against and verified to operate correctly under Microsoft Windows XP Service Pack 2.

RuggedExplorer must be installed and run with administrative privileges on a computer with an Ethernet network card. The network card must be configured to use TCP/IP and have a valid IPv4 address. A web browser is required to make use of the online help feature (accessed via help links within the software).

The installation program contains the RuggedExplorer application, integrated online help, PDF documentation, and all supporting software libraries required by the application. An Internet connection is not required to install and run RuggedExplorer.

Note

As part of the RuggedExplorer software installation, WinPcap (the Windows Packet Capture Library), is also installed. If WinPcap is already installed, its installation routine will ask whether to continue or to cancel the WinPcap installation. Selecting "Cancel" at this point cancels the reinstallation of WinPcap, and not the installation of RuggedExplorer.

1.5. Compatibility / Operating Requirements

RuggedExplorer is available in two different versions:

- The basic version of RuggedExplorer contains support for the RSH and TFTP protocols for remote command and file transfer.
- The **Encrypted** version additionally contains support for the SSH and SFTP protocols.

Note

*Please contact RuggedCom support in order to obtain a copy of the **Encrypted** version of RuggedExplorer.*

Note

*ROS has a three-digit version numbering system of the form: **X.Y.Z**, where:*

- ***X** represents the major revision number.*
- ***Y** represents the minor revision number.*
- ***Z** represents the patch level.*

The different versions of RuggedExplorer, and the different discovery methods it supports, have different ROS version requirements from devices that it is to discover and manage:

- RuggedExplorer has been verified to operate correctly with the latest patch level of each minor release since ROS v3.0.0.
- The Encrypted version requires ROS v3.5.3 or newer in order to make use of encrypted protocols.
- The Automatic Discovery mode requires RCDP support, which is present in ROS v3.7.0 and newer.

In addition, it is assumed that no VLANs (tagged or untagged) have been configured in the devices to be discovered and managed by RuggedExplorer. In other words, ROS devices must have default VLAN settings.

2. User Interface

2.1. Initialization

When RuggedExplorer™ is run for the first time on a computer system that has more than one network interface, it will prompt the user to select a network interface to use:

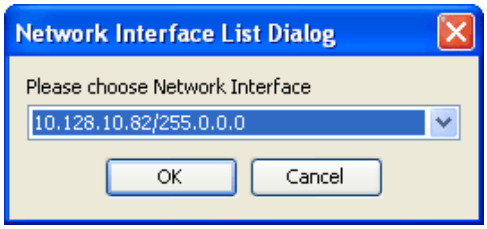


Figure 2.1. Network Interface List Dialog Box

If the computer system has only one network interface, this dialog box will not be displayed.

2.2. Main Window

The RuggedExplorer™ main window is displayed upon program initialization. RuggedExplorer configuration and control, device discovery, upload, download and configuration, are all accessed via buttons and menu items located in the main window. Devices discovered by RuggedExplorer are displayed in real time in the table that occupies most of the main window.

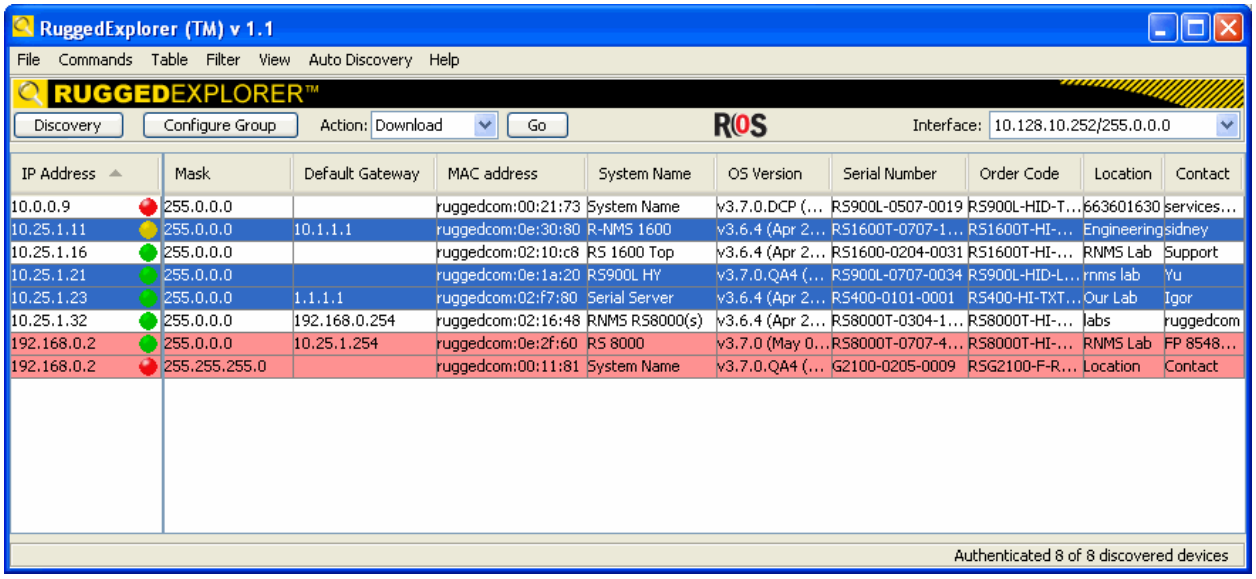

RuggedExplorer (TM) v 1.1
File Commands Table Filter View Auto Discovery Help
RUGGEDEXPLORER™
Discovery
Configure Group
Action: Download
Go
ROS
Interface: 10.128.10.252/255.0.0.0
IP Address Mask Default Gateway MAC address System Name OS Version Serial Number Order Code Location Contact
10.0.0.9 255.0.0.0 ruggedcom:00:21:73 System Name v3.7.0.DCP (... RS900L-0507-0019 RS900L-HID-T... 663601630 services...
10.25.1.11 255.0.0.0 10.1.1.1 ruggedcom:0e:30:80 R-NMS 1600 v3.6.4 (Apr 2... RS1600T-0707-1... RS1600T-HI-... Engineering sidney
10.25.1.16 255.0.0.0 ruggedcom:02:10:c8 RS 1600 Top v3.6.4 (Apr 2... RS1600-0204-0031 RS1600T-HI-... RNMS Lab Support
10.25.1.21 255.0.0.0 ruggedcom:0e:1a:20 RS900L HY v3.7.0.QA4 (... RS900L-0707-0034 RS900L-HID-L... rnms lab Yu
10.25.1.23 255.0.0.0 1.1.1.1 ruggedcom:02:f7:80 Serial Server v3.6.4 (Apr 2... RS400-0101-0001 RS400-HI-TXT... Our Lab Igor
10.25.1.32 255.0.0.0 192.168.0.254 ruggedcom:02:16:48 RNMS RS8000(s) v3.6.4 (Apr 2... RS8000T-0304-1... RS8000T-HI-... labs ruggedcom
192.168.0.2 255.0.0.0 10.25.1.254 ruggedcom:0e:2f:60 RS 8000 v3.7.0 (May 0... RS8000T-0707-4... RS8000T-HI-... RNMS Lab FP 8548...
192.168.0.2 255.255.255.0 ruggedcom:00:11:81 System Name v3.7.0.QA4 (... G2100-0205-0009 RSG2100-F-R... Location Contact
Authenticated 8 of 8 discovered devices

Figure 2.2. Main Window

2.2.1. Main Window Display

The main RuggedExplorer window consists chiefly of a list of discovered RuggedCom devices that is updated in real time. As devices are discovered, they are displayed in the list and sorted by IP address. Each row in the table contains information about the corresponding device.

2.2.1.1. Device Display Table

The display is separated into two panes:

- The **Status Pane**, on the left, includes only a column for IP Address and a Status Lamp Icon. The size of this column is static and does not allow resizing.
- The **Information Pane**, to the right, includes all the remaining information columns (see the list below).

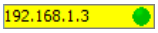
The Information Pane is customizable in several ways:

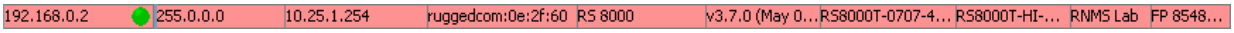
- Each column may be moved in relation to the others by clicking on the column title and dragging it left or right across the pane.
- The entire display may be sorted on the basis of any one of the columns (including the IP Address column). Clicking on a column title will sort the whole list in increasing order of the items in that column. Clicking again will sort in decreasing order.
- Each column may be resized by clicking and dragging the rightmost edge of a column title.
- Selected columns may be hidden altogether by disabling them in the View Menu. Note that the "MAC Address" column cannot be hidden since it is the only piece of data that is guaranteed to be unique among devices.

2.2.1.2. Color-coded Indicators

Row Color

The row containing the data for a given device is displayed in a different background color depending on its status:

- 

An IP address field displayed in a flashing yellow background indicates that the device has accepted the "Flash LEDs" command. This state persists until a "Stop flashing LEDs" command is issued or until it reaches its internal timeout (by default 5 minutes). This state is displayed at the same time as one of the others described below.
- 

Entries displayed in a red background have duplicate IP addresses. When the device's IP address has been reconfigured, its background will revert to plain white.
-

Entries displayed in a blue background have been selected for further manipulation. Device selection is made by clicking on an entry, holding down the Shift key and selecting a range of entries, holding down the Ctrl key and clicking on additional entries, in the standard Windows interface style. Details of what can be done with selected devices will be discussed in detail throughout this guide.

Status Lamp Icon

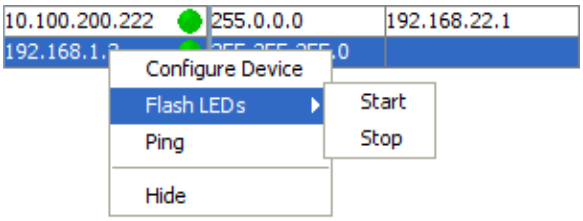
The Status Pane contains a lamp icon to the right of the IP address of the device, indicating the status of the device. Moving the mouse to pause over this icon will cause a "tool-tip" window to be dislpayed with additional status information. The status icon is displayed in one of three colors depending on the status of the device:

- 10.100.200.222 An IP address field displayed with a green lamp icon indicates that RuggedExplorer has successfully established communication with the device.
- 10.100.200.222 An IP address field displayed with a red lamp icon indicates that RuggedExplorer has not been able to establish communication with the device.
- 10.100.200.222 An IP address field displayed with a yellow lamp icon indicates that RuggedExplorer has detected some error condition on the device, for example, that a file transfer has failed.

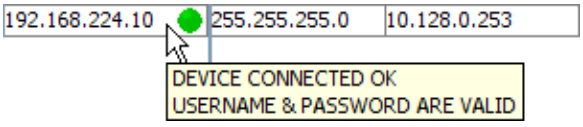
2.2.1.3. Operations on Table Entries

Device entries in the Device Display Table support several operations and shortcuts:

- **Clicking** on a device entry selects it for further operations using the Main Window Menu Bar or the Main Window Buttons.
- **Double-clicking** on a device entry brings up the Device Configuration dialog box.
- **Right-clicking** on a device entry brings up a pop-up menu:



  This pop-up menu contains yet another link to the Device Configuration dialog box, the ability to start or stop flashing LEDs on the device, and a single "ping" test to verify that the device is reachable via IP.
- **Hovering** over an IP address field displays a tool-tip message containing a brief summary of the corresponding device's status, for example:



2.2.1.4. Main Window Display Columns

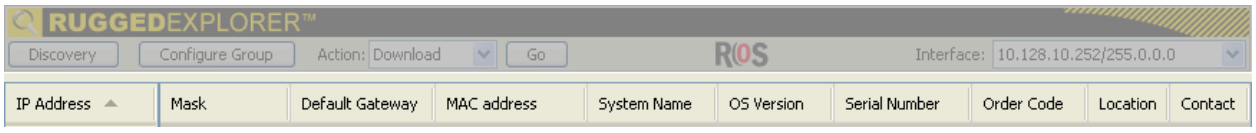


Figure 2.3. Main Window Display Columns

RuggedExplorer's main window displays columns of information captured from a device when the device is first discovered.

IP Address The IP address of the discovered device. RuggedExplorer can discover devices with duplicate IP addresses when they are discovered using the Auto Discovery method. Devices with duplicate IP addresses will be highlighted in red to visually differentiate them from unique IP addresses. This is the only fixed column on the main window, meaning that it cannot

be moved from its location. The information in this column can be modified by RuggedExplorer.

Mask The IP address mask of the discovered device. The information in this column can be modified by RuggedExplorer.

Default Gateway The default IP gateway of the discovered device. The information in this column can be modified by RuggedExplorer and may be blank.

MAC Address The MAC address of the discovered device. This is a fixed value and therefore this column is not modifiable by RuggedExplorer.

System Name The configured system name of the discovered device. This column could contain the default value of the device ("System Name") or any string that has been configured. The information in this column can be modified by RuggedExplorer.

OS Version This column will display the current running version of ROS on the discovered device. The information in this column cannot be modified by RuggedExplorer.

Serial Number The unique serial number assigned to this device by RuggedCom at the factory. The information in this column cannot be modified by RuggedExplorer.

Order Code The order code of this device as set by by RuggedCom at the factory. The information in this column cannot be modified by RuggedExplorer.

Location The configured location string of the discovered device. This column could contain the default value of the device ("Location") or any string that has been configured. The information in this column can be modified by RuggedExplorer.

Contact The configured contact information of the discovered device. This column could contain the default value of the device ("Contact") or any string that has been configured. The information in this column can be modified by RuggedExplorer.

2.2.2. Main Window Buttons

Figure 2.4. Main Window Buttons

Several buttons and controls are located in a row above the main display window. These provide rapid and convenient access to the most commonly required functions of RuggedExplorer.

Discovery Clicking **Discovery** on the main window launches the Automatic and Manual device discovery processes. Please refer to Device Discovery for more detail.

Configure Device / Group This button is sensitive to context:

- Configure Device is displayed when no discovered devices are selected.
- Configure Device is displayed when a single discovered device is selected. Clicking this button displays the Device Configuration dialog box.

- Configure Group is displayed when multiple discovered devices are selected. Clicking this button displays the Group Device Configuration dialog box.

Action

The **Action** section on the main window gives options for the file transfer and maintenance features of RuggedExplorer. The pull-down menu has three options:

- Upload - Upload files from RuggedExplorer to one or more ROS devices.
- Download - Download files from one or more ROS devices to RuggedExplorer.
- Maintenance - Gives the following three options:
  - Clear logs
  - Reset device
  - Load factory defaults

Interface

The **Interface** list on the main window is used to select the network interface to be used by RuggedExplorer for network discovery and all device access except SSH. The interface selection may be changed at any time without the need to restart RuggedExplorer.

2.2.3. Main Window Menu Bar

File Menu

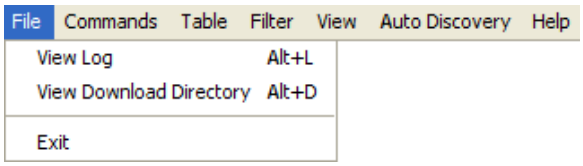


Figure 2.5. File Menu

View Log Open RuggedExplorer's log file in a text editor.

View Download Directory Open the download directory, into which RuggedExplorer writes files downloaded from discovered devices.

Exit Terminate RuggedExplorer.

Commands Menu

Figure 2.6. Commands Menu

As with the buttons on the main window, some items in the **Commands** menu are relevant only when a device is selected in the list. When more than one device is selected in the list, some menu items change name and function. These special cases are noted below.

Rescan	Rescan all discovered devices and update the parameters displayed in the main window.
Configure Device / Group	This menu item is displayed as **Configure Device** if only one device is highlighted in the main window, and opens the Device Configuration dialog box. If more than one device is highlighted in the main window, the menu item is displayed as **Configure Group**, and opens the Group Device Configuration dialog box.
Flash LEDs	The Flash LEDs menu selection will start and stop a visual identifier on the selected devices. This visual identification is in the form of LEDs flashing on the selected devices. This option is not available for devices discovered using the manual discovery mechanism.
Ping	Ping a single device to see if it is reachable. This menu item is only displayed if only one device is highlighted in the main window. Note that ping is unreliable in certain IP addressing situations, but if Automatic Discovery was used to discover the device, it is still accessible using RuggedExplorer.

Table Menu

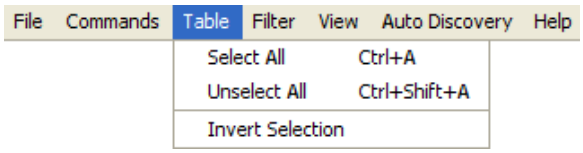


Figure 2.7. Table Menu

Select All	Select (highlight) all devices displayed in the main window.
Unselect All	Unselect (remove the highlights) from all selected devices.
Invert Selection	Invert selection will select all currently unselected devices and unselect all currently selected devices as seen on the main window.

Filter Menu

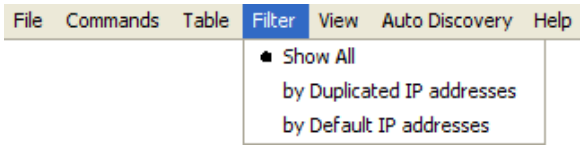


Figure 2.8. Filter Menu

The **Filter** menu controls the display of discovered devices in the main window. Only one of the three following filters is selected at once.

Show All	Display all discovered devices.
by Duplicated IP addresses	Display only devices with duplicate IP address settings.

by Default IP addresses — Display only devices with the default IP address set. Note that ROS devices ship with a default IP address of 192.168.0.1.

View Menu

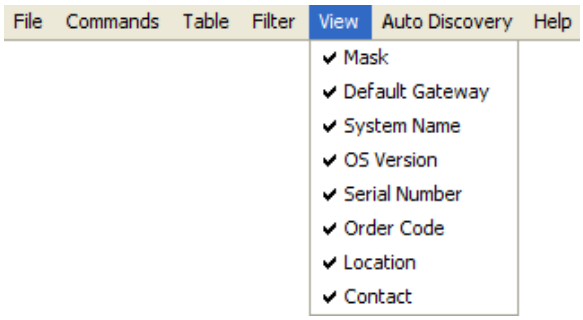


Figure 2.9. View Menu

The settings in the **View** menu select the fields that are displayed for each discovered device in the main window. Clicking on an item in the view menu toggles its state. A check mark beside the item indicates that a column for the corresponding field will be displayed in the main window.

- Mask
- Default Gateway
- System Name
- OS Version
- Serial Number
- Order Code
- Location
- Contact

Auto Discovery Menu

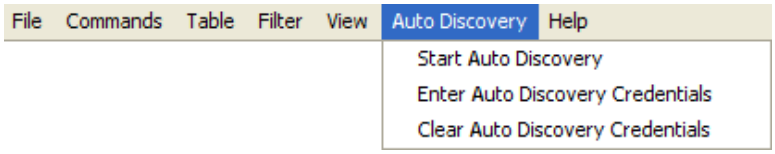


Figure 2.10. Auto Discovery Menu

RuggedExplorer is capable of automatically discovering devices using the RuggedCom Discovery Protocol (RCDP), an Ethernet-based protocol that allows RuggedExplorer to discover and manage devices irrespective of their IP network configuration. At the time of writing, only ROS-based devices running ROS version 3.7.0 or greater have support for RCDP.

Start Auto Discovery — Starts the automatic discovery.

Enter Auto Discovery Credentials — Allows a user to enter user name and password credentials to validate RuggedExplorer on the target devices. As many credentials can be entered as required. The user names and passwords entered are kept secure in RuggedExplorer and not

	retained by the application after RuggedExplorer is shut down. Credentials can be entered at any time, even after discovery is run, to display devices found by RuggedExplorer.
Clear Auto Discovery Credentials	Clicking on this menu entry will clear all the credentials known by RuggedExplorer.

Help Menu

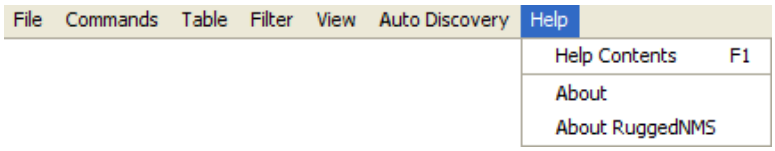


Figure 2.11. Help Menu

Help Contents	Display the HTML format of this User Guide.
About	Display brief information about RuggedExplorer.
About RuggedNMS	Display the RuggedNMS web site, http://www.ruggednms.com, in a web browser.

2.3. Device Discovery

RuggedExplorer supports two device discovery mechanisms:

- **Automatic Discovery** uses the RuggedCom Discovery Protocol™ (RCDP™) to discover devices running version 3.7.0 of ROS or newer.
- **Manual Discovery** uses TCP/IP to find devices running ROS versions older than 3.7.0. The manual discovery process is optional and is enabled by specifying an IP address range to scan for devices.

2.3.1. Auto Discovery

The Auto Discovery mechanism is started directly from the Auto Discovery Menu or in parallel with a Manual Discovery. It relies only on having an Ethernet connection to the ROS-based devices to be discovered. Devices may have nothing more than factory settings, and require no TCP/IP configuration.

2.3.1.1. Auto Discovery Access Configuration

RuggedExplorer attempts to authenticate itself with every device that it discovers in order to access device parameters. It uses default authentication parameters to access ROS-based devices whose authentication parameters have not been changed from factory defaults.

In order to be able to access devices whose authentication parameters have been configured away from factory defaults, RuggedExplorer must be provided with authentication credentials for those devices. Multiple sets of user name / password credentials may be configured in RuggedExplorer for use during the Auto Discovery process. Several sets of authentication credentials may be added to RuggedExplorer using the **Auto Discovery Access** dialog box, accessible by selecting **Enter Auto Discovery Credentials** from the Auto Discovery Menu.

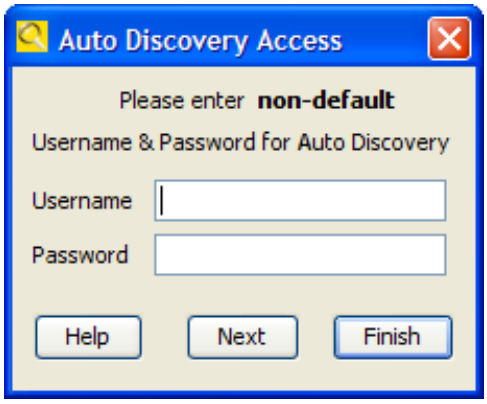


Figure 2.12. Auto Discovery Access Dialog Box

Username	A user name to add to RuggedExplorer's database to be used during Auto Discovery.
Password	A password to add to RuggedExplorer's database to be used during Auto Discovery.
Next	Clicking **Next** adds the user name and password currently in the dialog and clears the dialog box's contents to be ready to accept another set of credentials.
Finish	Clicking **Finish** adds the user name and password currently in the dialog and exits the dialog box.

All authentication credentials added to RuggedExplorer using this dialog box may be deleted at once by selecting **Clear Auto Discovery Credentials** from the Auto Discovery Menu.

2.3.2. Manual Discovery

Both the Automatic and Manual device discovery processes are initiated using the **Manual Device Discovery** dialog box, which is accessible from the Main Window Buttons. The Automatic Discovery mechanism is run as a part of every discovery process, and has no configurable parameters. The Manual Discovery process must be configured (via the specification of an IP range using this dialog box) in order to enable it to run.

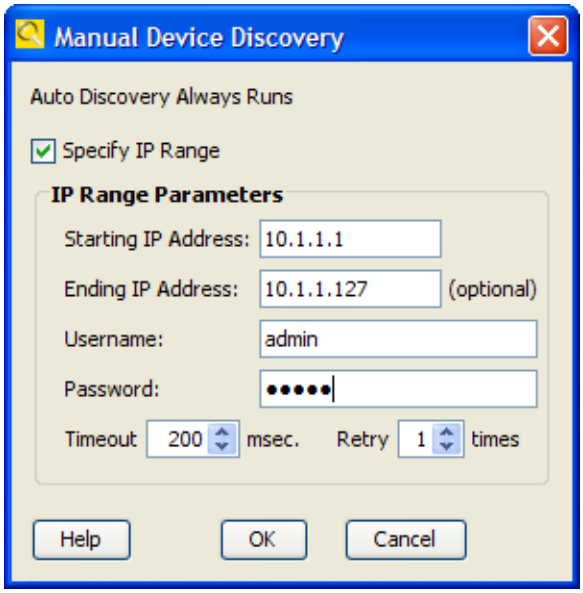


Figure 2.13. Device Discovery Dialog Box

Specify IP Range	Checking the box will enable Manual Discovery. If this box is not checked, then only the Auto Discovery will run.
Starting IP Address	Starting IP address for the ping sweep.
Ending IP Address	Ending IP address for the ping sweep. If this field is left empty, then only one device will be pinged (the Starting IP Address).
Username	The user name that RuggedExplorer will use when validating itself on discovered devices.
Password	The password that RuggedExplorer will use when validating itself on discovered devices.
Timeout	The ping timeout value used by Manual Discovery.
Retry	The number of ping retries before RuggedExplorer determines that no device exists at a given IP address.
OK	Clicking OK will start the discovery process. Devices discovered via RCDP will be entered directly into the Device Display Table. Note that if a given device is discovered via TCP/IP and also via RCDP, then RCDP will take precedence and will be used for subsequent access to the device.
Cancel	Exit the dialog box and do not perform a discovery process.

Note

Since ROS allows ten failed password attempts before disallowing logins, please do not perform multiple manual device discovery runs on the same IP range in order to accomodate different sets of authentication credentials.

If possible, try to group the IP ranges to discover by common authentication credentials. In the extreme, in which every device had different credentials, it would be necessary to perform a manual discovery for each device, in an IP range restricted to each device.

Note

Discovering devices in IP address ranges that are not on the locally connected network requires that a default gateway be correctly configured on the PC running RuggedExplorer.

2.3.2.1. IP Address Range Discovery/Validation

If a manual device discovery is configured to run (by specifying **IP Range Parameters** in the Manual Device Discovery Dialog Box), the **IP Address Range Discovery/Validation** dialog box will report its progress.

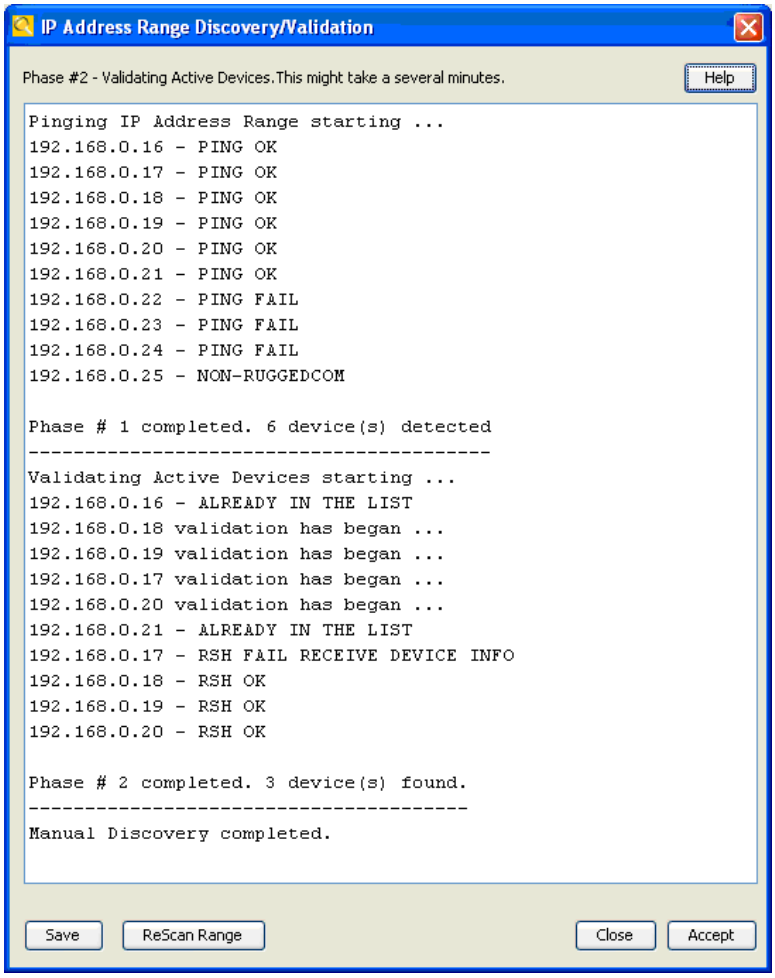

IP Address Range Discovery/Validation
Phase #2 - Validating Active Devices.This might take a several minutes.
Help
Pinging IP Address Range starting ...
192.168.0.16 - PING OK
192.168.0.17 - PING OK
192.168.0.18 - PING OK
192.168.0.19 - PING OK
192.168.0.20 - PING OK
192.168.0.21 - PING OK
192.168.0.22 - PING FAIL
192.168.0.23 - PING FAIL
192.168.0.24 - PING FAIL
192.168.0.25 - NON-RUGGEDCOM
Phase # 1 completed. 6 device(s) detected
Validating Active Devices starting ...
192.168.0.16 - ALREADY IN THE LIST
192.168.0.18 validation has began ...
192.168.0.19 validation has began ...
192.168.0.17 validation has began ...
192.168.0.20 validation has began ...
192.168.0.21 - ALREADY IN THE LIST
192.168.0.17 - RSH FAIL RECEIVE DEVICE INFO
192.168.0.18 - RSH OK
192.168.0.19 - RSH OK
192.168.0.20 - RSH OK
Phase # 2 completed. 3 device(s) found.
Manual Discovery completed.
Save
ReScan Range
Close
Accept

Figure 2.14. IP Address Range Discovery/Validation

The manual discovery process is carried out in two phases:

- During Phase 1, RuggedExplorer determines which devices in the selected IP address range respond to IP "ping" requests.
- During Phase 2, RuggedExplorer probes those devices it discovered during phase 1 to verify that it can access them.

2.3.3. Rescanning Discovered Devices

RuggedExplorer can be made to update its information about the devices it has already discovered by selecting **Rescan** from the Commands Menu. If a device was discovered using RCDP (Auto Discovery), it will be rescanned using RCDP. If it was discovered using TCP/IP (Manual Discovery), it will be rescanned using TCP/IP.

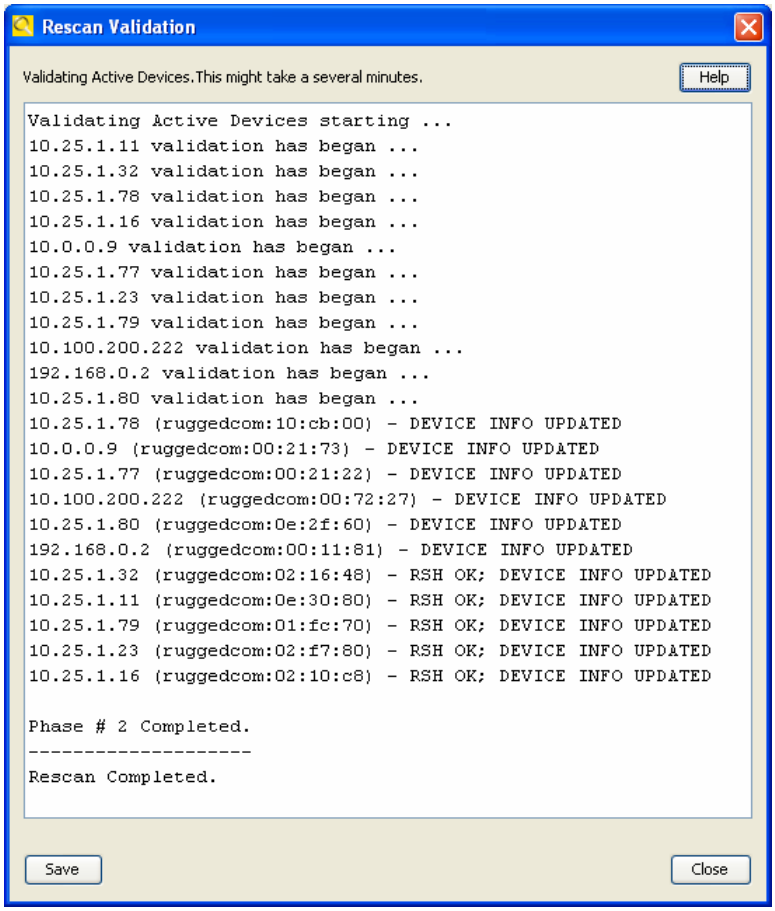

Rescan Validation
Validating Active Devices.This might take a several minutes.
Help
Validating Active Devices starting ...
10.25.1.11 validation has began ...
10.25.1.32 validation has began ...
10.25.1.78 validation has began ...
10.25.1.16 validation has began ...
10.0.0.9 validation has began ...
10.25.1.77 validation has began ...
10.25.1.23 validation has began ...
10.25.1.79 validation has began ...
10.100.200.222 validation has began ...
192.168.0.2 validation has began ...
10.25.1.80 validation has began ...
10.25.1.78 (ruggedcom:10:cb:00) - DEVICE INFO UPDATED
10.0.0.9 (ruggedcom:00:21:73) - DEVICE INFO UPDATED
10.25.1.77 (ruggedcom:00:21:22) - DEVICE INFO UPDATED
10.100.200.222 (ruggedcom:00:72:27) - DEVICE INFO UPDATED
10.25.1.80 (ruggedcom:0e:2f:60) - DEVICE INFO UPDATED
192.168.0.2 (ruggedcom:00:11:81) - DEVICE INFO UPDATED
10.25.1.32 (ruggedcom:02:16:48) - RSH OK; DEVICE INFO UPDATED
10.25.1.11 (ruggedcom:0e:30:80) - RSH OK; DEVICE INFO UPDATED
10.25.1.79 (ruggedcom:01:fc:70) - RSH OK; DEVICE INFO UPDATED
10.25.1.23 (ruggedcom:02:f7:80) - RSH OK; DEVICE INFO UPDATED
10.25.1.16 (ruggedcom:02:10:c8) - RSH OK; DEVICE INFO UPDATED
Phase # 2 Completed.
Rescan Completed.
Save
Close

Figure 2.15. Rescan Validation

2.4. Device Configuration

Depending on whether one or multiple discovered devices are selected in the main window Device Display Table, either the **Configure Device** or the **Configure Group** button will be displayed, respectively. A different dialog box is presented in each case, as detailed in the next two sections.

2.4.1. Single Device Configuration

RuggedExplorer allows a user to modify certain configuration parameters on a device. The single device dialog box below shows the parameters available for configuration.

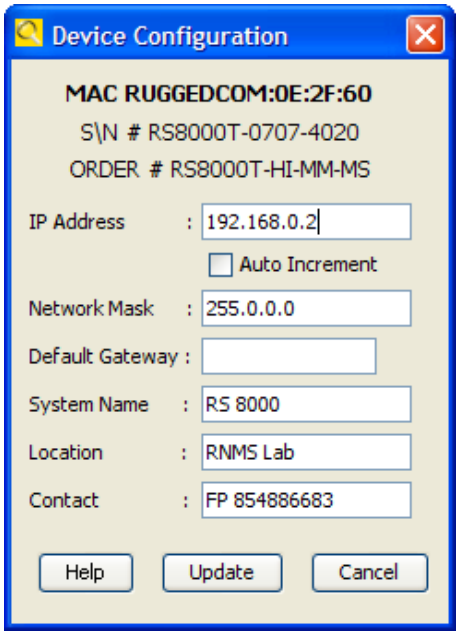


Figure 2.16. Device Configuration Dialog Box

IP Address	The IP address to be configured.
Auto Increment	If this box is checked, the IP address will be automatically incremented next time this dialog box is opened.
Network Mask	The network mask to be configured.
Default Gateway	The default gateway to be configured.
System Name	The system name to be configured.
Location	The location to be configured.
Contact	The contact information to be configured.
Update	Clicking Update will commit the requested configuration changes to the selected device.
Cancel	Clicking Cancel will exit this dialog, discarding any specified configuration changes.

Note

Attempting to configure an IP address that is already in use elsewhere in the network will cause RuggedExplorer to report an error.

2.4.2. Group Device Configuration

RuggedExplorer allows a user to select multiple devices in the user interface for group configuration. When multiple devices are selected and Group Configuration is chosen, the dialog box seen below is displayed. Group configuration enables the automated configuration of the selected devices.

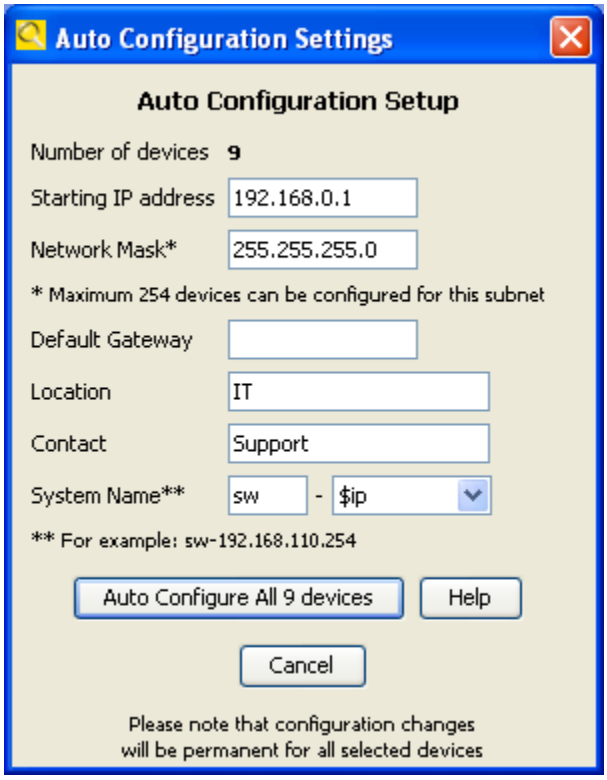


Figure 2.17. Group Configuration Dialog Box

Number of Devices — This field displays the number of devices that were selected in the main window for configuration.

Starting IP address — The selected devices will be assigned consecutive addresses starting with this IP address. IP addresses in the sequence that are detected to already be in use are simply skipped over and not used.

Network Mask — The specified mask will be applied to all selected devices.

Default Gateway — The specified default gateway will be applied to all selected devices.

Location — The specified location will be applied to all selected devices.

Contact — The specified contact information will be applied to all selected devices.

System Name — This field is used as a template to assign a different system name to each discovered device. The first field is a static prefix to every device name and the second field is selected from a pull-down for the variable, template-based portion of the system name. Two templates are available:

- $ip - the IP address of the device.
- $sequence - a sequence number, automatically incremented for each device.

A sample system name based on the specified prefix and template is displayed below the **System Name** field.

Auto Configure All Devices	Clicking on this button will start the autoconfiguration process.
Cancel	Clicking Cancel will exit this dialog, discarding any specified configuration changes.

2.5. Device Control

RuggedExplorer is capable of performing a selected set of operations on devices it has discovered. One or more devices may be selected by highlighting them in the Main Window Device Display Table. The following operations, described in subsequent sections, are performed on all highlighted devices:

- file downloads
- file uploads
- system management commands

2.5.1. Download

The File Download dialog box presents a choice of files that may be downloaded from selected ROS-based devices, along with the option to create an archive file of all downloaded files.

RuggedExplorer downloads files from multiple selected devices concurrently.

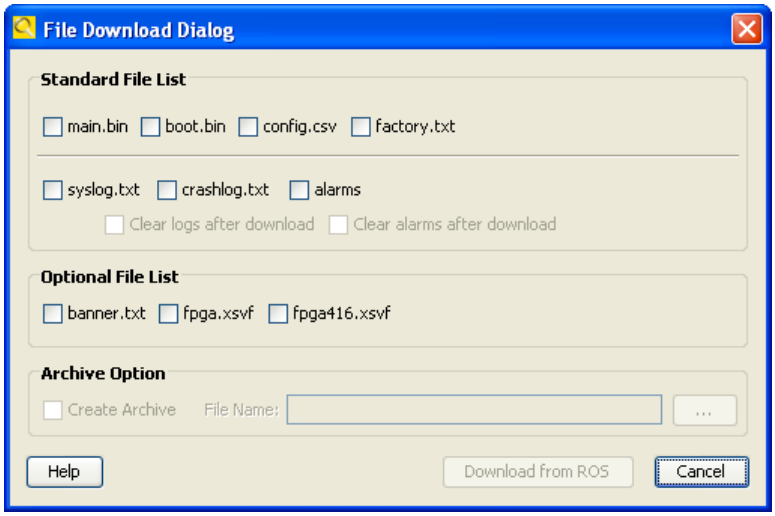


Figure 2.18. File Download Dialog Box

Files To Download

The files that may be downloaded from a ROS device are:

main.bin	- the main ROS firmware image file
boot.bin	- the ROS bootloader firmware (very infrequently updated)
config.csv	- the ROS system configuration file

syslog.txt	- log of system events
crashlog.txt	- log of debilitating system events
alarms	- list of active alarms
banner.txt	- the optional ROS login banner text file
banner.txt	- the optional ROS login banner text file
fpga.xsvf	- FPGA programming image file
fpga416.xsvf	- Second FPGA programming image file specific to the RS416

The following files may optionally be erased from the device after having been downloaded. Note that selecting "Clear logs after download" forces the download of both "syslog.txt" and "crashlog.txt" since these may not be deleted individually.

- syslog.txt
- crashlog.txt
- alarms

Downloaded Files

Downloaded files are placed in subdirectories of the download directory (by default, this is the "downloads" subdirectory of the RuggedExplorer installation directory).

Text files (configuration, logs, etc.) downloaded from a particular device are placed in subdirectories whose name contains the device's IP address. Every downloaded text file will be saved with an extended file name including a date stamp and a numeric identifier to guarantee that each downloaded file is unique. For example, the system log (syslog.txt) from a device might be saved with the following file name:
`Syslog-20090101-000101.txt`

Binary files are saved in the root of the download directory. Duplicate files are not downloaded; that is, if multiple devices have the same firmware version, the firmware file will only be downloaded once. Binary files will be saved with extended file names including the firmware image name and version. For example, the ROS main firmware image (main.bin) from a device running ROS version 3.6.1 would be saved with the following file name:
`ROS-CF52_Main_v3-6-1.bin`

When the "Create Archive" option is selected, a unique archive file name is automatically generated and presented in the "File Name" field, for example:
`downloads\archive-20090802-181011.zip`

This file name can be overridden by editing the field. The complete set of downloaded files is archived to this file name.

2.5.2. Upload

The File Upload dialog box presents a choice of files on ROS devices that may be uploaded for replacement.

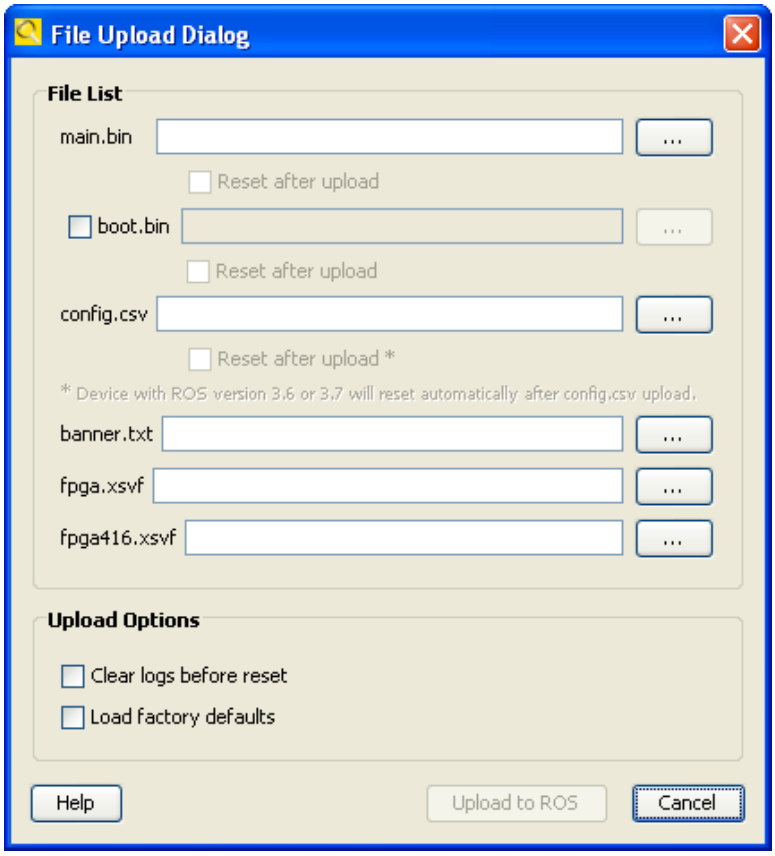


Figure 2.19. File Upload Dialog Box

The files that may be replaced via a file upload on a ROS device are:

main.bin - the main ROS firmware image file
boot.bin - the ROS bootloader firmware (very infrequently updated)
config.csv - the ROS system configuration file
banner.txt - the optional ROS login banner text file
fpga.xsvf - FPGA programming image file
fpga416.xsvf - Second FPGA programming image file specific to the RS416

RuggedExplorer takes a conservative approach to uploading firmware and configuration files to many ROS-based devices at a time.

When a file upload operation is initiated on multiple devices with the reset option enabled, RuggedExplorer begins by selecting a "pilot device" on which to test the complete operation before committing to performing the same operations on the whole list of selected devices. The pilot device is defined to be the selected device with the lowest numeric IP address.

If more than one file is chosen for upload at a time, they are be uploaded in the following sequence:

1. boot.bin
2. main.bin

3. config.csv
4. other files

Note that for some of these files, it will be necessary to reset the device prior to uploading the next file. RuggedExplorer will automatically select the corresponding **Reset after upload** check box accordingly. The pilot / remainder sequence described above is used for `boot.bin` and `main.bin`. The `config.csv` file is uploaded sequentially, and never concurrently.

If an error occurs while uploading files to multiple ROS devices, RuggedExplorer will exclude the affected device from the processing list but will continue to process the other devices in the list.

Two more options are available for the file upload process:

- Selecting **Clear logs before reset** erases the contents of `syslog.txt` and `crashlog.txt` on the ROS devices to which files are being uploaded before they are reset.
- Selecting **Load factory defaults after reset** causes factory default setttings to be restored to the ROS devices to which files are being uploaded after they are reset.

Note

ROS devices running version 3.6 or 3.7 automatically reset upon receiving an upload of a new system configuration file, `config.csv`.

2.5.3. Maintenance

RuggedExplorer performs maintenance operations on multiple selected devices sequentially.

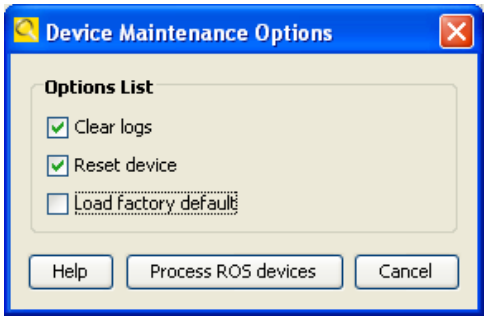


Figure 2.20. Device Maintenance Dialog Box

Clear logs	Delete all log files on the device.
Reset device	Perform a device reset.
Load factory defaults	Set all configurable device parameters to their factory default settings.

2.5.4. Progress Indication

After initiating a download, upload, or maintenance command for selected devices, a dialog box will be displayed indicating the progress relative to each device. Note that entries in green indicate devices

that RuggedExplorer is accessing the corresponding device using encrypted (SSH) communications and entries in blue indicate devices that it is accessing using unencrypted (RSH) communications.

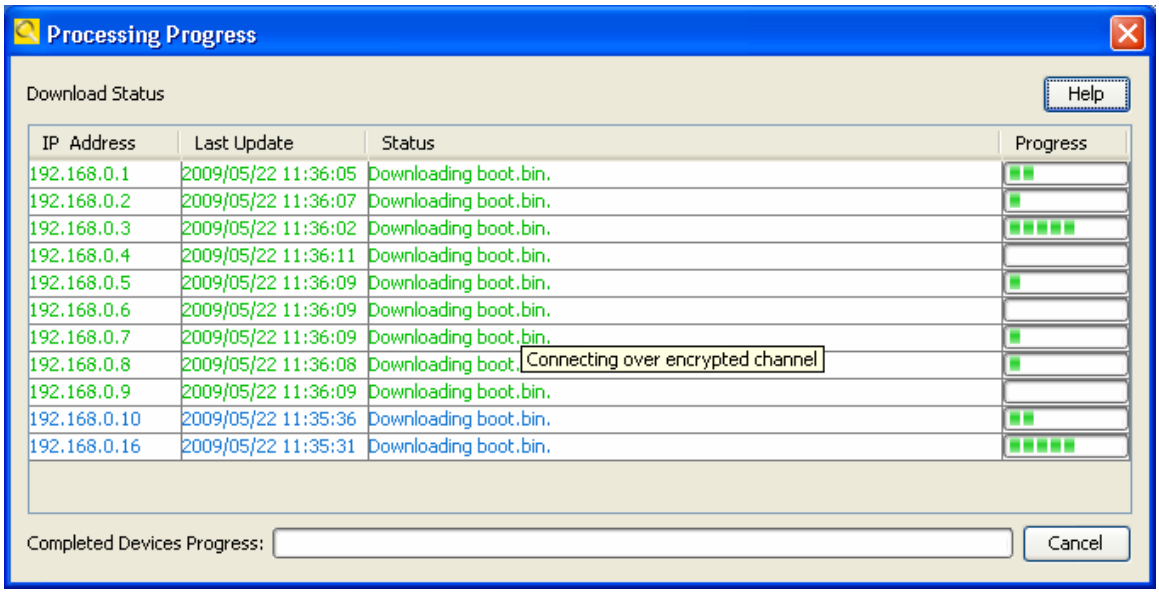


Figure 2.21. Progress Dialog Box (Processing in Progress)

Note the **Completed Devices Progress** bar, which indicates the proportion of devices for which RuggedExplorer has completed processing. Moving the mouse over any given entry causes a tool-tip window to be displayed, indicating whether the device is being accessed using encryption.

Clicking the **Cancel** button aborts the multi-device process.

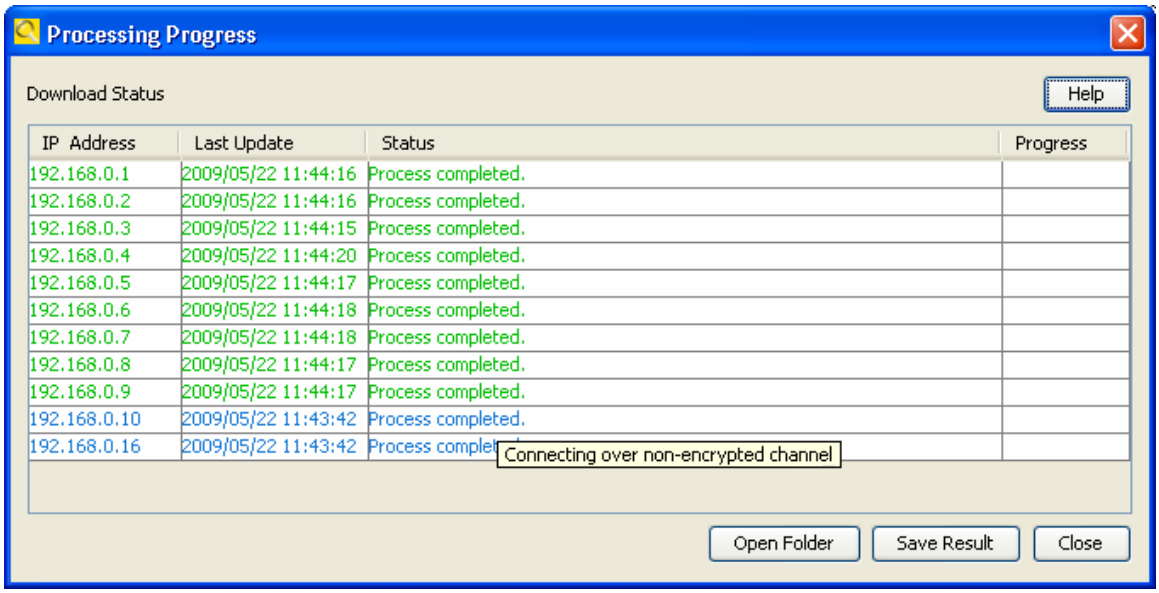


Figure 2.22. Progress Dialog Box (Processing Complete)

Clicking **Save Result** saves RuggedExplorer log files for each processed device.

Open Folder opens a file browser in the file download directory.

Note

Uploading the Export version of ROS to a device that is currently running the Secure version will result in a lapse in RuggedExplorer's communication with the device. It is recommended to avoid mixing ROS versions in this way.

Double-clicking on an entry in the **Processing Progress** dialog box brings up a window displaying the log for the corresponding device. The same information displayed here is also reflected in the `RuggedExplorer.log` file, although there it is interleaved with log data for all other devices.

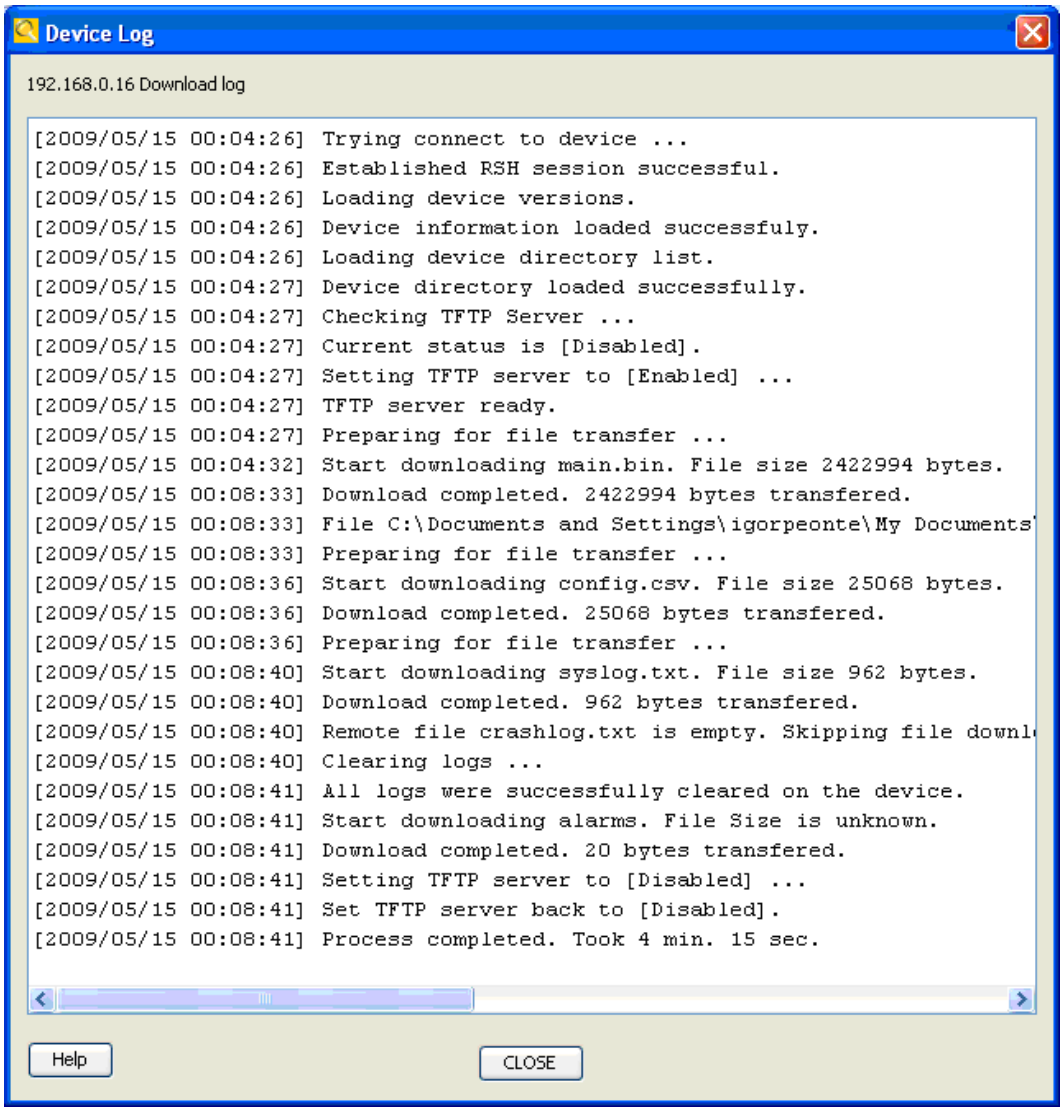

Device Log
192.168.0.16 Download log
[2009/05/15 00:04:26] Trying connect to device ...
[2009/05/15 00:04:26] Established RSH session successful.
[2009/05/15 00:04:26] Loading device versions.
[2009/05/15 00:04:26] Device information loaded successfuly.
[2009/05/15 00:04:26] Loading device directory list.
[2009/05/15 00:04:27] Device directory loaded successfully.
[2009/05/15 00:04:27] Checking TFTP Server ...
[2009/05/15 00:04:27] Current status is [Disabled].
[2009/05/15 00:04:27] Setting TFTP server to [Enabled] ...
[2009/05/15 00:04:27] TFTP server ready.
[2009/05/15 00:04:27] Preparing for file transfer ...
[2009/05/15 00:04:32] Start downloading main.bin. File size 2422994 bytes.
[2009/05/15 00:08:33] Download completed. 2422994 bytes transfered.
[2009/05/15 00:08:33] File C:\Documents and Settings\igorpeonte\My Documents
[2009/05/15 00:08:33] Preparing for file transfer ...
[2009/05/15 00:08:36] Start downloading config.csv. File size 25068 bytes.
[2009/05/15 00:08:36] Download completed. 25068 bytes transfered.
[2009/05/15 00:08:36] Preparing for file transfer ...
[2009/05/15 00:08:40] Start downloading syslog.txt. File size 962 bytes.
[2009/05/15 00:08:40] Download completed. 962 bytes transfered.
[2009/05/15 00:08:40] Remote file crashlog.txt is empty. Skipping file downl
[2009/05/15 00:08:40] Clearing logs ...
[2009/05/15 00:08:41] All logs were successfully cleared on the device.
[2009/05/15 00:08:41] Start downloading alarms. File Size is unknown.
[2009/05/15 00:08:41] Download completed. 20 bytes transfered.
[2009/05/15 00:08:41] Setting TFTP server to [Disabled] ...
[2009/05/15 00:08:41] Set TFTP server back to [Disabled].
[2009/05/15 00:08:41] Process completed. Took 4 min. 15 sec.
Help
CLOSE

Figure 2.23. Device Log

3. Theory Of Operation

This chapter provides information on how RuggedExplorer™ operates from a network perspective.

3.1. Device Discovery Methods

RuggedExplorer™ uses two different methods to discover ROS® devices for management.

3.1.1. Automatic (RuggedCom Discovery Protocol™-based) Device Discovery

The Automated Discovery method is based on a proprietary Layer 2 Ethernet protocol called the RuggedCom Discovery Protocol™ (RCDP™). ROS version 3.7.0 devices running RCDP actively listen for RCDP discovery messages, sent as Ethernet multicasts, from RuggedExplorer. A ROS device must acknowledge the reception of a discovery message from RuggedExplorer to register itself with the management application and establish a session.

Upon completion of the session registration between RuggedExplorer and ROS, RuggedExplorer can begin management of the device. Since RCDP messages are based on Ethernet and its addressing mechanism, and do not make any use of IP, RuggedExplorer can communicate with ROS devices that have not been assigned an IP address. As a result, RuggedExplorer can be used to configure the IP address on ROS devices irrespective of their network configuration. Moreover, since RCDP is not dependent on IP, it can be used to discover and display devices that have conflicting IP addresses and allow a user to reconfigure these devices.

To discover new devices added to the network or devices that were not initially discovered, RuggedExplorer periodically sends rediscovery messages. Only ROS devices that did not previously complete the registration process with RuggedExplorer will respond to the rediscovery messages to control network traffic. The rediscovery process runs periodically after RuggedExplorer sends the initial discovery message.

3.1.2. Manual (TCP/IP-based) Device Discovery

The Manual Discovery method uses a ping sweep to discover ROS devices that have a valid IP address and do not support RCDP. The manual discovery process has 2 phases:

- Phase 1 requires a user to select the discovery dialogue and enter a starting and ending IP address. Clicking the OK button causes RuggedExplorer to start the pinging process which will sequentially go through the list of IP addresses and records IP addresses that respond.
- Phase 2 attempts to log on to the devices that responded to a ping with the provided user name and password to assess whether it is a ROS device or not. At the end of phase 2, a list of devices is available for management by RuggedExplorer.

3.1.3. RCDP Versus TCP/IP Discovery Comparison

The following table provides a brief comparison of the two discovery mechanisms used by RuggedExplorer:

	RCDP	Ping Sweep
Discovery method	Ethernet messages	ICMP Ping messages
Rediscovery	Send periodically	Not supported
Display configuration parameters	Supported	Supported
Visual identification	Supported (based on device capabilities)	Not supported
Change configuration parameters	Supported	Supported
Determine support for encryption when discovered	No	Yes (for version that supports encryption only)

3.2. Security Considerations

In order for RuggedExplorer to authenticate itself to the devices it connects to, it must be given the user names and passwords for these devices.

Note

For security reasons, user name and password device credentials are not stored permanently by RuggedExplorer.

Automatic Discovery requires a user to enter the credential pairs through the user interface using the Auto Discovery Access Configuration menu. Manual Discovery asks for device credentials when the ping sweep is being configured. The device credentials for each discovery type are only used by that type meaning that the information is not shared. To manually discover devices with different credentials, the ping sweep must be re-run with a different user name and password. Doing this does not discard any previously discovered devices unless a user chooses to remove them. All user names and passwords entered via the user interface are discarded when RuggedExplorer is shut down.

RCDP does not send user names and passwords in its messages so this information remains secure. The non-encrypted version of RuggedExplorer does send user names and passwords in clear text and would be readable by someone snooping on the line. The encrypted version of RuggedExplorer does not expose any sensitive information.

Note

RCDP is enabled by default on ROS devices running version 3.7.0 or newer.

3.3. Duplicate Instance Detection

While RuggedExplorer runs, it monitors the network for other nodes that may be attempting to perform RCDP-based discovery, since the presence of more than one active RCDP master on the network is disruptive to the correct operation of the Automatic Discovery mechanism and of subsequent command and control of RCDP-compliant devices.

If RuggedExplorer detects another instance running on the network, it issues a warning similar to the following:

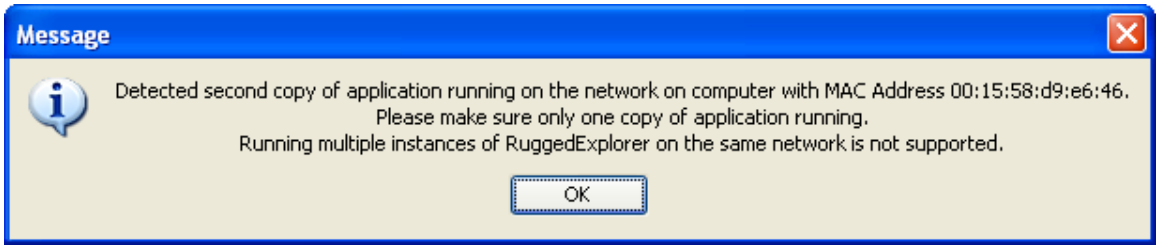

Message
Detected second copy of application running on the network on computer with MAC Address 00:15:58:d9:e6:46.
Please make sure only one copy of application running.
Running multiple instances of RuggedExplorer on the same network is not supported.
OK

Figure 3.1. Detecting Another Instance Of RuggedExplorer On The LAN

Note

In order to be able to detect other instances on the network, RuggedExplorer places the network interface in ***promiscuous mode****.*

If RuggedExplorer detects another instance running on the same computer, it issues a different warning:

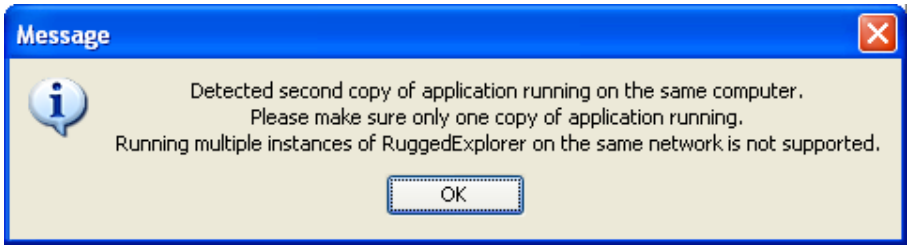

Message
Detected second copy of application running on the same computer.
Please make sure only one copy of application running.
Running multiple instances of RuggedExplorer on the same network is not supported.
OK

Figure 3.2. Detecting Another Instance Of RuggedExplorer On The Same Computer

Appendix A. RuggedExplorer.ini Configuration File

The `RuggedExplorer.ini` file, located in the RuggedExplorer™ installation directory, stores program defaults, parameters specified and discovered at run-time. It is also possible to edit the file using a regular ASCII text editor in order to explicitly configure certain aspects of RuggedExplorer.

The file has a simple structure:

- `[section name]` - denotes the start of one of the configuration file sections.
- `;` - A line beginning with a semicolon is a comment.
- `variable = value` - A line of this form assigns a value to one of RuggedExplorer's configurable variables.

In the following sections, the different sections of `RuggedExplorer.ini` are presented as they appear in the file. The configurable variables for each section are listed, preceded by comment fields describing the function of each one.

A.1. Auto Configuration Parameters

```
[auto_config]
; Last network mask used for Auto-Configuration process
net_mask =

; Last default gateway used for Auto-Configuration process
default_gw =

; Last starting IP address used for Auto-Configuration process
start_ip =
```

A.2. Logging Parameters

```
[log]
; Maximum size of the log file
file_max_size = 5000

; Destination directory for log file. If unspecified, this defaults
; to the directory in which the RuggedExplorer executable resides
directory_name =
```

A.3. General Parameters

```
[general]
; Preferred communication protocol. Valid values are "ssh" (encrypted)
; or "rsh" (unencrypted)
pref_comm = ssh

; Default administrator password used by the Layer 2
; auto discovery protocol
admin_pwd = admin
```

```
; Last interface used by RuggedExplorer. If this is empty,
; RuggedExplorer will present a drop-down list with all interfaces.
; upon start-up
management_ip =

; Show a disclaimer when running the Encrypted version.
secure_ver_warning = true

; Destination directory for device file downloads.
; If unspecified, this defaults to the directory in which the
; RuggedExplorer executable resides.
downloads = downloads

; Whether to make use of SSH for encrypted communication with
; discovered devices. Note that this has no impact on the
; unencrypted version of RuggedExplorer.
secure_mode = false

; Default administrator user name used by the Layer 2
; auto discovery protocol
admin_username = admin
```

Appendix B. RuggedExplorer™ Software License

RuggedExplorer Software

End User License Terms and Conditions

THIS RUGGEDCOM RUGGEDEXPLORER SOFTWARE END USER LICENSE TERMS AND CONDITIONS ("LICENSE") IS A CONTRACT BETWEEN YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) AND RUGGEDCOM FOR THE RUGGEDCOM RUGGEDEXPLORER SOFTWARE. YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE INSTALLING THIS RUGGEDCOM RUGGEDEXPLORER SOFTWARE. THE RUGGEDEXPLORER SOFTWARE, ANY RELATED DOCUMENTATION, AND ANY UPDATES, ENHANCEMENTS, OR SUPPLEMENTS THERETO THAT MAY BE PROVIDED TO YOU BY RUGGEDCOM DURING THE TERM OF THIS LICENSE, ARE COLLECTIVELY REFERRED TO HEREIN AS THE "RUGGEDEXPLORER SOFTWARE". INSTALLING THIS RUGGEDEXPLORER SOFTWARE INDICATES YOUR ACCEPTANCE OF THESE TERMS AND CONDITIONS OF THIS LICENSE. IF YOU DO NOT AGREE WITH THESE TERMS AND CONDITIONS, YOU SHOULD NOT USE AND PROMPTLY RETURN THE RUGGEDEXPLORER SOFTWARE TO RUGGEDCOM FOR YOUR MONEY REFUND.

B.1. LICENSE

B.1.1.

RuggedCom grants you the following personal, non-transferable and nonexclusive rights, provided that you comply with the terms and conditions of this License:

B.1.1.1.

You may: (a) install and use the RuggedExplorer Software only on one (1) single computer at any time (a "computer" being hereby defined as one central processing unit and associated peripheral equipment, all at one location); and (b) copy the RuggedExplorer Software into any machine-readable or printed form for backup purposes only in support of your own use of the RuggedExplorer Software on a single computer.

B.1.2.

You must NOT interfere with, remove, obstruct, cover, delete, or change the copyright and other proprietary notices of RuggedCom on any copy of all or any portion of the RuggedExplorer Software, and all such copies shall be subject to all the terms and conditions of this License.

B.1.3.

YOU MAY NOT USE, COPY OR TRANSFER THE RUGGEDEXPLORER SOFTWARE OR ANY COPY THEREOF, IN WHOLE OR IN PART, EXCEPT AS EXPRESSLY PROVIDED IN THIS LICENSE. IF YOU TRANSFER POSSESSION OF ANY COPY OF THE RUGGEDEXPLORER SOFTWARE TO ANOTHER PARTY, YOUR LICENSE IS AUTOMATICALLY TERMINATED. YOU

SHALL NOT DISTRIBUTE, PUBLICLY DISPLAY OR PERFORM, OR EITHER MODIFY, ALTER OR CREATE DERIVATIVE WORKS OF THE RUGGEDEXPLORER SOFTWARE.

B.1.4.

RuggedCom reserves all rights not expressly granted to you under this License.

B.2. TITLE AND OWNERSHIP

B.2.1.

You acknowledge and agree that all right, title and interest in the RuggedExplorer Software is solely and exclusively owned by RuggedCom, and you shall acquire no rights in the RuggedExplorer Software other than as expressly granted in this License. The RuggedExplorer Software is protected by Canadian, United States and international copyright laws and other intellectual property and proprietary laws.

B.2.2.

You acknowledge and agree that the RuggedExplorer Software constitute valuable proprietary assets of RuggedCom, embodying substantial creative efforts and significant expenditures of time and money. You hereby agree to observe complete confidentiality with respect to the RuggedExplorer Software, including but not limited to the following:

B.2.2.1.

You agree to only permit authorised access to the RuggedExplorer Software and you shall ensure that anyone who is permitted access to the RuggedExplorer Software is made aware of and agrees to abide by the obligations imposed on you under this License.

B.2.2.2.

You agree not to attempt to disassemble, decompile or otherwise reverse-engineer the RuggedExplorer Software.

B.2.2.3.

You agree: (a) not to make unauthorized copies of all or any portion of the RuggedExplorer Software; (b) not to sell, rent, sublicense, give or otherwise disclose, distribute or transfer to any third party any portion of the RuggedExplorer Software or copies thereof; and (c) not to install the RuggedExplorer Software on a service bureau or other remote access system whereby persons or entities other than you can obtain the benefits of use of the RuggedExplorer Software;

B.2.3.

You agree that in the event of an unauthorized reproduction, transfer or disclosure of any part of or all of the RuggedExplorer Software, RuggedCom and the RuggedCom Licensors will suffer immediate

and irreparable harm for which, after such occurrence, neither shall have an adequate remedy at law, and you therefore agree that injunctive or other equitable relief will be a fair and appropriate remedy to restrain or prevent any such reproduction, transfer or disclosure, either threatened or actual.

B.2.4.

The provisions of this Section 2 shall survive any termination of this License.

B.3. LIMITED WARRANTY

B.3.1.

EXCEPT AS OTHERWISE PROVIDED IN THIS SECTION 3, THE RUGGEDEXPLORER SOFTWARE IS PROVIDED "AS IS" AND RUGGEDCOM DISCLAIMS, TO THE FULL EXTENT PERMITTED BY LAW, ALL OTHER REPRESENTATIONS, COVENANTS AND WARRANTIES, (EXPRESS OR IMPLIED), STATUTORY, OR OTHERWISE, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THERE IS NO EXPRESS OR IMPLIED WARRANTY OF TITLE OR NONINFRINGEMENT WITH REGARD TO THE RUGGEDEXPLORER SOFTWARE. THE ENTIRE RISK AS TO THE PERFORMANCE OF THE RUGGEDEXPLORER SOFTWARE IS WITH YOU.

B.3.2.

RuggedCom does not warrant that the functions contained in the RuggedExplorer Software will meet your requirements or that the operation of the RuggedExplorer Software will be uninterrupted or error free.

B.3.3.

RuggedCom warrants the diskette(s) or other media type on which the RuggedExplorer Software is furnished to be free from defects in materials and workmanship under normal use for a period of 1 year (356 days) from the Shipping Date as evidenced by a copy of your RuggedCom Purchase Order.

B.4. LIMITATION OF REMEDIES

B.4.1.

In the event of breach of the limited warranty in Section 3.3, RuggedCom's entire, combined and aggregate liability and your exclusive remedy for all occurrences shall be strictly limited to:

B.4.1.1.

The replacement of any diskette or other media type not meeting RuggedCom's "Limited Warranty" and which is returned to RuggedCom with a copy of your RuggedCom Purchase Order; or

B.4.1.2.

If RuggedCom is unable to deliver a replacement diskette or other media type which is free of defects in materials or workmanship, you may terminate this License by returning the RuggedExplorer Software and any money paid to RuggedCom for the RuggedExplorer Software Fee will be refunded.

B.4.2.

IN NO EVENT WILL RUGGEDCOM BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY INDIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL, OR PUNITIVE DAMAGES (INCLUDING, BUT NOT LIMITED TO, ANY LOST PROFITS, LOST SAVINGS, BUSINESS INTERRUPTION OR OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE RUGGEDEXPLORER SOFTWARE EVEN IF RUGGEDCOM, HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, THE AGGREGATE LIABILITY OF RUGGEDCOM, WILL BE LIMITED TO THE AMOUNT ACTUALLY PAID BY YOU TO RUGGEDCOM FOR THE RUGGEDEXPLORER SOFTWARE RUGGEDCOM ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR RUGGEDCOM ANY OTHER LIABILITIES IN CONNECTION WITH THE SALE OF RUGGEDCOM PRODUCTS. YOU AGREE THAT THIS EXCLUSION OF LIABILITY PROVISION IS FAIR AND REASONABLE IN THE COMMERCIAL CIRCUMSTANCES OF THIS LICENSE.

B.5. INDEMNIFICATION

B.5.1. Indemnification In Favour Of Yourself

B.5.1.1.

Notwithstanding Section 4.2, RuggedCom hereby agrees to indemnify, hold harmless, and defend you, provided that you make a claim against RuggedCom for such indemnity, from all claims, proceedings, liabilities, actions, suits, judgments and orders, based on a claim that your use of the RuggedExplorer Software (except to the extent caused by components not provided by RuggedCom) infringes a patent, copyright or any other intellectual property right, provided that you notify RuggedCom as soon as reasonably practical of any such claim, demand or cause of action for which you will require such indemnification from RuggedCom. You will provide RuggedCom with reasonable information and assistance for RuggedCom to defend such claim, demand, or cause of action.

B.5.1.2.

Section 5.1.1 shall not apply if: 1) if you breach section 2.2.3; or 2) if you altered, modified, tampered with or changed any part or component of the RuggedExplorer Software.

B.5.1.3.

Should the RuggedExplorer Software become, or in RuggedCom's opinion be likely to become, the subject of a claim of infringement of a patent, copyright or any other intellectual property right, RuggedCom shall have the right to either: (i) procure for you, at no cost to yourself, the right to continue

to use the RuggedExplorer Software; or (ii) replace or modify the RuggedExplorer Software at no cost to you to make the RuggedExplorer Software non-infringing, provided that the equivalent functionality is performed by the replacement or modified RuggedExplorer Software. If neither of these options is available to RuggedCom on commercially reasonable terms, RuggedCom may terminate the right to use and/or distribute the RuggedExplorer Software.

B.5.2. Indemnification In Favour Of RuggedCom

You agree to hereby indemnify and saves harmless RuggedCom, and its directors, officers, agents, stakeholders, and employees from all and against any and all claims, demand, litigation, harm, injury, losses, liabilities, judgments, damages and costs (including taxes) and all related expenses, including reasonable legal fees and disbursements and costs of investigation, litigation and settlement, together with interest and penalties ("Claim"), suffered by RuggedCom, as a result of, or arising out of or in connection with, the following: (a) your use of or inability to use the RuggedExplorer Software; (b) your breach of or failure to, arising in negligence or otherwise, in whole or in part, perform any of the obligations, representations, warranties or covenants under this License; (c) your violation of any applicable laws and regulations; (d) any death or personal injury by reason of any act or omission, whether negligent or otherwise, to the extent caused by you in connection with this License; and (e) your malicious, fraudulent (including fraudulent misrepresentation) or criminal conduct (whether by act or omission). If a Claim is made or threatened against RuggedCom in respect of a Claim for which you owe an indemnity obligation pursuant to this Section 5.2, and if RuggedCom intends to seek indemnity with respect thereto, RuggedCom shall notify you of such Claim and it shall be your duty to vigorously defend such claim or action without cost or expense to RuggedCom or its directors, officers, agents, stakeholders, or employees.

B.6. TERMINATION

The rights granted under this License are effective until terminated. You may terminate this License at any time by destroying all copies of the RuggedExplorer Software in your possession, and providing written notice of such termination and destruction to RuggedCom. This License will terminate automatically without notice if you violate any of the terms and conditions of this License. You agree upon such termination to promptly destroy all copies of the RuggedExplorer Software in your possession and to certify in writing to RuggedCom that such action has been taken.

B.7. GOVERNING LAW

In the event an action is commenced to enforce a party's right under this License, the prevailing party in such action shall be entitled to recover its costs and reasonable lawyer fees. You agree that the closest and most convenient connection for this License, and the transactions contemplated thereby, is with the Province of Ontario, Canada and you agree that this License will be governed by and construed in accordance with the sole and exclusive laws of the province of Ontario and the federal laws of Canada applicable therein, without giving effect to the principles of conflicts of law, and excluding the body of law applicable to choice of law and excluding the United Nations Convention on Contracts for the International Sale of Goods, if applicable. You irrevocably submit to the non-exclusive jurisdiction of the courts of Ontario for the purpose of any suit, action or other proceeding arising out of this License or the subject matter hereof. If RuggedCom is obligated to go to court, to enforce any of its rights against you, or to collect any fees from you, you agree to reimburse RuggedCom for its legal fees, costs and disbursements if RuggedCom is successful.

B.8. ASSIGNMENT

None of your rights, duties or obligations under this License may be sold, sublicensed, assigned or otherwise transferred, except as expressly provided in this License, without the prior written consent of RuggedCom, and any attempt to do so without RuggedCom's consent is void.

B.9. RESTRICTED RIGHTS

The RuggedExplorer Software and related documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the United States Government or any instrumentality thereof, is subject to restrictions as set forth in subparagraph (c)(1)(ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of the Commercial Computer Software -- Restricted Rights at 48 CFR 52.227-19, as applicable.

B.10. ACKNOWLEDGEMENT

YOU ACKNOWLEDGE THAT: (a) YOU HAVE READ THIS ENTIRE LICENSE AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS; (b) THIS LICENSE IS THE COMPLETE AND EXCLUSIVE STATEMENT OF THE UNDERSTANDING AND CONTRACT BETWEEN YOU AND RUGGEDCOM AND SUPERSEDES ANY AND ALL PRIOR ORAL OR WRITTEN COMMUNICATIONS RELATING TO THE SUBJECT MATTER HEREOF; AND (c) THIS LICENSE MAY NOT BE MODIFIED, AMENDED OR IN ANY WAY ALTERED EXCEPT IN WRITING AND SIGNED BY BOTH YOU AND RUGGEDCOM.

Index

A
Address and Status Pane, 11

C
Compatibility, 8
Configuration, 21
Control, 24

D
Discovery, 17
  Auto Discovery Access Configuration, 17
  Automatic, 17
  Manual, 18
Download, 24

F
Features, 7

I
Information Pane, 11
Initialization, 10
Installation Notes, 8
Introduction, 7

M
Main Window
  Buttons, 13
  Dialog, 10
  Menu Bar, 14
Maintenance, 27

O
Operating Requirements, 8

P
Purpose, 7

U
Upload, 25
Use Cases, 7